

**12 APRIL 2002**



**Communications and Information**

**REQUESTING UNCLASSIFIED NETWORK  
USER AND E-MAIL ACCOUNTS (PA)**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>

---

OPR: 36 CS/SCBB (2Lt Charles Mack)

Certified by: 36 CS/CC (Lt Col Susan Pardo)

Pages: 5

Distribution: F

---

This instruction implements AFI 33-119, *Electronic Mail (E-Mail) Management and Use*, AFI 33-129, *Transmission of Information Via the Internet* and AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*. It establishes policies and procedures for the creation and management of Andersen Domain unclassified user and e-mail accounts. This publication does not apply to Air National Guard (ANG) or Air Force Reserve personnel.

This publication prescribes 36ABW11, Unclassified Network User and E-mail Account Application, which requires the collection and or maintenance of information protected by the Privacy Act of 1974, Public Law 99-474, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of this information. The 36ABW 11 contains the appropriate PA statement.

**1. Procedures.** All requirements for unclassified user and e-mail accounts will be identified by using 36 ABW Form 11, **Unclassified Network User and E-Mail Account Application**. The following are responsibilities and procedures for accomplishing the form:

1.1. The Requesters (users) will:

1.1.1. Contact their unit workgroup manager (WM) or supervisor/sponsor to obtain the 36 ABW Form 11.

1.1.2. Contact their unit computer security (COMPUSEC) manager or unit WM for access to Network Users License Training computer based training (CBT).

1.1.3. Satisfactorily complete the required modules of the IA internet-based training course.

1.1.4. Print CBT results and provide the printout to your unit COMPUSEC manager

1.1.5. Complete 36 ABW Form 11, Section I, Blocks 1 through 12 and Section IV, Blocks 1 and 2.

1.1.6. Contact unit WM for assistance with identifying required user and e-mail groups necessary for mission accomplishment.

- 1.2. The user's Supervisor or Sponsor (if the person is a contractor) will:
  - 1.2.1. Ensure user understands and adheres to policies, procedures, and practices outlined in the IA Internet-based training course. In the event the user does not adhere to these policies, the supervisor will report the event to the unit WM. See paragraph 3.1. for further details.
  - 1.2.2. Complete 36 ABW Form 11, Section II, Blocks 1 through 6.
  - 1.2.3. Complete 36 ABW Form 11, Section IV, Blocks 3 and 4.
  - 1.2.4. Ensure 36 ABW Form 11, Sections I and II and Sections IV through VI are completed before form is dispatched to the Help Desk.
- 1.3. The Unit WM will:
  - 1.3.1. Provide requester (user) with 36 ABW Form 11 (if necessary).
  - 1.3.2. Provide access to the IA Internet-based training course and, if necessary, assist in printing the completion results.
  - 1.3.3. Identify and list domain user and e-mail groups user must be added to. The domain user groups will be listed on the 36 ABW Form 11, Section I, Block 11, and the e-mail groups will be listed in Section I, Block 12.
  - 1.3.4. Ensure Sections V and VI are completed.
  - 1.3.5. Provide the 36 ABW Form 11 to the Help Desk electronically (scanned), in hard copy, or via FAX.
  - 1.3.6. In the event a user does not adhere to domain user policies, take an active part in correcting the situation. See Section 3.1 for further details.
  - 1.3.7. Perform selected account maintenance actions (i.e., unlocking accounts, correcting user names, resetting/changing account passwords) after being designated one of the Lead WMs for his or her unit and completing necessary WM training.
- 1.4. The Unit Security Manager will:
  - 1.4.1. Verify user's National Agency Check (NAC).
  - 1.4.2. Complete 36 ABW Form 11, Section V, Blocks 1 through 6.
- 1.5. The Unit COMPUSEC Manager will:
  - 1.5.1. Provide access to AFI 33-119, *Electronic Mail (E-Mail) Management and Use* and AFI 33-129, *Transmission of Information Via the Internet*.
  - 1.5.2. Verify satisfactory completion of IA Internet-based training course.
  - 1.5.3. Complete 36 ABW Form 11, Section VI, Blocks 1 through 4.
  - 1.5.4. In the event a user does not adhere to domain user policies, assist and advise the WM in correcting the situation. See paragraph 3.1 for further details.
- 1.6. The 36 CS Help Desk will:
  - 1.6.1. Create the domain user account.
  - 1.6.2. Create the e-mail account (if applicable).

- 1.6.3. Complete 36 ABW Form 11, Section III, Blocks 1 through 10.
- 1.6.4. Add user to approved domain and e-mail groups (if applicable) and record assigned groups on 36ABW Form 11, Section III, Block 9.
- 1.6.5. Record the date user and e-mail accounts were deleted on 36 ABW Form 11, Section III, Blocks 4 and 8 respectively.
- 1.6.6. Perform domain and e-mail account maintenance (i.e., unlocking accounts, correcting user names, resetting/changing account passwords, adding user to new user or e-mail groups, etc).
- 1.6.7. Keep completed 36 ABW Form 11 on file at the Help Desk IAW AFMAN 37-139, *Records Disposition Schedule*.

**2. Account Lockout Procedures.** In the event of account lockout there are three options open to users:

- 2.1. The user may contact one of his or her unit's Lead WMs and have him or her unlock the user's account after user provides positive identification.
- 2.2. If one of the unit's Lead WMs is not available, the user may contact one of the other WMs in the unit and have him or her verify identification. The WM can then call the Help Desk stating they have verified the user's identification and the Help Desk will unlock the account.
- 2.3. The user may contact the Help Desk to have his or her account unlocked. Help Desk personnel will require positive identification (in person) before they can unlock the account.

**3. Denial Authority.** The unit WM or Network Control Center (NCC) may suspend a user's license when deemed necessary in the interest of network security. Actions inconsistent with licensing principles include, but are not limited to: failure to maintain an acceptable level of proficiency on a critical program; actions that threaten the security of a network or a governmental communications system; actions that may result in damage or harm to a network or governmental communications system; or actions that constitute unauthorized use under the provisions of AFI 33-119, *Electronic Mail (E-Mail) Management and Use*, or AFI 33-129, *Transmission of Information Via the Internet*.

- 3.1. If a user engages in conduct inconsistent with the licensing principles or the policies of the network, implement the following:
  - 3.1.1. The witness of the conduct will report it to the unit WM.
  - 3.1.2. The unit WM will:
    - 3.1.2.1. Work with the unit COMPUSEC Manager to ensure any insecurities posed by the conduct are mitigated.
    - 3.1.2.2. Determine whether this is a minor or major infraction and if suspension and/or remedial training is called for. The seriousness of the offense, the willingness and ability of the user to correct undesired conduct, and the counsel of the user's supervisor will determine whether the infraction is major or minor.
    - 3.1.2.3. **For minor infractions:** handle remedial training locally according to AFI 33-115V2 paragraph 4.3 through 4.3.2 or call the Help Desk to open a trouble ticket for remedial training for the user.

3.1.2.4. **For major infractions:** call the Help Desk and open a ticket for remedial training for the user.

3.1.3. Upon receiving the call from the unit WM, the Help Desk personnel will:

3.1.3.1. **For minor infractions:** set the user's account to expire in 30 days from the time the infraction trouble ticket is opened. At the end of the 30 days, if the user has not satisfactorily completed remedial training, the account will be locked out and their network license suspended until remedial training is completed.

3.1.3.2. **For major infractions:** lock out the user's account immediately, thus immediately suspending the user's license. The license will remain suspended until the Wing IA office notifies Help Desk personnel to unlock the account. This notification will occur after the user has completed the required remedial training.

3.1.3.2.1. In the notes field of the user's account, the Help Desk technician will write "**Remedial Training Required. See Ticket #####**", where ##### is the initial trouble ticket number associated with the infraction.

3.1.3.2.2. Report the open ticket to the Wing Information Assurance (IA) Office and the Network Security Office.

3.1.4. The Wing IA Office will:

3.1.4.1. Determine and develop tailored remedial training for the user depending upon the type of offense.

3.1.4.2. Contact the user's supervisor and/or unit WM to set an appointment to administer the training to the user.

3.1.4.3. Conduct training for the user.

3.1.4.4. Once the user has satisfactorily completed remedial training, notify the Help Desk to lose the ticket and request the expiration date be cleared from the user's account.

3.1.4.5. Notify the supervisor and/or unit WM of the completion of the remedial training.

3.2. Network access suspension is a non-punitive action and the suspension alone, as opposed to the underlying conduct, may not provide the basis for adverse action. Actions dictated herewith are provided for use when deemed necessary in the interest of information operations and to educate network users of that interest. Other adverse actions towards the offending user are the responsibility of the unit. As with any disciplinary issue, it may be advisable to seek counsel from other agencies on base, such as the 36 ABW Legal Office, the 36th Security Forces Squadron, or the Air Force Office of Special Investigations.

**4. Out-Processing.** When users depart for a TDY greater than 90 days or depart for PCS, they must inform the Help Desk for account maintenance and/or deletion within 5 workdays prior to departure. If user is going TDY, the Help Desk will mark the user's account TDY. This will prevent the account from being deleted.

**5. Form Prescribed:** 36 ABW Form 11, **Unclassified Network User and E-Mail Account Application.**

BERNARD H. FULLENKAMP, Colonel, USAF  
Commander, 36th Air Base Wing